Entiers de Gauss

Marc Lorenzi

2 janvier 2026

1 Introduction

L'ensemble des *entiers de Gauss* est $\mathbb{G} = \{a + ib : a, b \in \mathbb{Z}\}$. On vérifie facilement que $\mathbb{G}$ est un sous-anneau de $\mathbb{C}$ contenant $\mathbb{Z}$. Remarquons que $\mathbb{G}$ est également stable par passage au conjugué : pour tout $x = a + ib \in \mathbb{G}$, $\overline{x} = a - ib \in \mathbb{G}$.

Définition 1. Pour tout $x \in \mathbb{G}$, la *norme* de x est $N(x) = x\overline{x}$.

Si $x = a + ib$ où $a, b \in \mathbb{Z}$, on a $N(x) = a^2 + b^2 \in \mathbb{N}$. La norme étant un module au carré, on a immédiatement que $N(x) = 0$ si et seulement si $x = 0$. Également, pour tous $x, y \in \mathbb{G}$, $N(xy) = N(x)N(y)$. La norme va avoir un rôle important dans tout l'article. Elle joue dans l'arithmétique de l'anneau $\mathbb{G}$ le rôle de la valeur absolue dans l'anneau $\mathbb{Z}$.

Proposition 1. *Les inversibles de* $\mathbb{G}$ *sont* ± 1 *et* $\pm i$.

Démonstration. Soit $x = a + ib \in \mathbb{G}$. Supposons x inversible, d'inverse y. On a $xy = 1$. En passant aux normes, $N(x)N(y) = 1$. Or, $N(y)$ et $N(y)$ sont des entiers naturels, donc $N(x) = N(y) = 1$. On a ainsi $a^2 + b^2 = 1$. Les seuls couples d'entiers solutions de cette équation sont $(\pm 1, 0)$ et $(0, \pm 1)$. Ainsi, $x = \pm 1$ ou $x = \pm i$. Inversement, ces 4 entiers de Gauss sont inversibles, d'inverses ± 1 et $\mp i$. □

Nous noterons dorénavant

$$\mathbb{U} = \{1, i, -1, -i\}$$

2 Divisibilité

2.1 Diviseurs, multiples

Définition 2. Soient $x, y \in \mathbb{G}$. x *divise* y (ou y est *multiple* de x) lorsqu'il existe $z \in \mathbb{G}$ tel que $y = xz$.

Nous noterons $x \,|\, y$ lorsque x divise y. Dans le cas contraire, nous noterons $x \nmid y$. Une ambiguïté apparaît. Si $x, y \in \mathbb{Z}$ et que x divise y, parlons-nous de divisibilité dans $\mathbb{Z}$ ou dans $\mathbb{G}$? En fait,

il y a équivalence. Si x divise y dans $\mathbb{Z}$, il existe $z \in \mathbb{Z}$ tel que $y = zx$. Comme $z \in \mathbb{Z} \subset G$, x divise aussi y dans $\mathbb{G}$. Inversement, si x divise y dans $\mathbb{G}$, il existe $z \in \mathbb{G}$ tel que $y = xz$. Posons $z = a + ib$ où $a, b \in \mathbb{Z}$. On a

$$y = y + i0 = xz = ax + ibx$$

Par unicité de l'écriture des nombres complexes, $y = ax$, donc x divise y dans $\mathbb{Z}$.

Proposition 2. *La relation de divisibilité est réflexive et transitive. Pour tous $x, y \in \mathbb{G}$, x divise y et y divise x si et seulement si il existe $w \in \mathbb{U}$ tel que $y = wx$.*

Démonstration. Soit $x \in \mathbb{G}$. On a $x = 1x$ donc $x|x$, d'où la réflexivité.

Soient $x, y, z \in \mathbb{G}$. Supposons que $x|y$ et $y|z$. Soient $w, t \in \mathbb{G}$ tels que $y = wx$ et $z = ty$. On a $z = (tw)x$ donc $x|z$, d'où la transitivité.

Soient $x, y \in \mathbb{G}$. Supposons que $x|y$ et $y|x$. Soient $w, t \in \mathbb{G}$ tels que $y = wx$ et $x = ty$. Si $x = 0$, alors $y = w0 = 0$, donc $y = 1x$. Supposons $x \neq 0$. On a $x = (tw)x$ donc $1 = tw$. Ainsi, $w \in \mathbb{U}$. Inversement, supposons qu'il existe $w \in \mathbb{U}$ tel que $y = wx$. On a $x|y$ mais aussi, comme $x = w^{-1}y$, $y|x$. □

Définition 3. Les entiers de Gauss x et y sont *associés* lorsque x divise y et y divise x.

Notons $\mathcal{R} = \{z = a + ib \in \mathbb{C}^* \text{ tels que } \mathrm{Re}(z) > 0 \text{ et } \mathrm{Im}(z) \geq 0\}$.

Proposition 3. *Pour tout $x \in \mathbb{G}$ non nul, un et un seul des associés de x appartient à $\mathcal{R}$.*

Démonstration. Soit $x \in \mathbb{G} \setminus \{0\}$. Soit $\theta = \arg(x) \in]-\pi, \pi]$. Les associés de x ont pour arguments $\theta + k\pi/2$ où $k \in \mathbb{Z}$. L'appartenance à $\mathcal{R}$ équivaut à

$$0 \leq \theta + k\frac{\pi}{2} < \frac{\pi}{2}$$

ou encore

$$-\frac{2}{\pi}\theta \leq k < -\frac{2}{\pi}\theta + 1$$

Il existe un seul entier k vérifiant cette propriété, à savoir

$$k = \left\lfloor -\frac{2}{\pi}\theta \right\rfloor$$

□

2.2 Division euclidienne

Tout comme $\mathbb{Z}$, l'anneau $\mathbb{G}$ peut être muni d'une division euclidienne.

Proposition 4. *Soient $a, b \in \mathbb{G}$ tels que $b \neq 0$. Il existe $(q, r) \in \mathbb{G}^2$ tel que $a = bq + r$ et $N(r) < N(b)$.*

Remarquons que l'on n'affirme pas l'unicité du couple (q, r). Dans la suite, nous parlerons tout de même *du* quotient et *du* reste de la division euclidienne de a par b. On peut lever l'ambiguïté en choisissant pour q et r les deux entiers de Gauss définis dans la démonstration ci-dessous.

Démonstration. Soit $z = u + iv = a/b \in \mathbb{C}$. La partie réelle u et la partie imaginaire v de z sont deux rationnels. Posons $x = \lfloor u + 1/2 \rfloor$ et $y = \lfloor v + 1/2 \rfloor$. On a $x, y \in \mathbb{Z}$, $|x - u| \leq 1/2$ et $|y - v| \leq 1/2$. Soit $q = x + iy \in \mathbb{G}$. On a

$$|z - q|^2 = (x - u)^2 + (y - v)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

De là, en multipliant par $N(b)$,

$$N(a - bq) \leq \frac{1}{2} N(b)$$

En posant $r = a - bq$, on a le résultat. On a même un peu mieux , puisque $N(r) \leq N(b)/2$. □

L'anneau $\mathbb{G}$ est ainsi un *anneau euclidien*. Il est donc aussi *principal*. La preuve est classique, c'est l'objet du paragraphe suivant.

2.3 Les idéaux de $\mathbb{G}$

Proposition 5. *Les idéaux de $\mathbb{G}$ sont les ensembles $a\mathbb{G}$ où $a \in \mathbb{G}$.*

Démonstration. Il est clair que pour tout $a \in \mathbb{G}$, $a\mathbb{G}$ est un idéal de $\mathbb{G}$. Inversement, soit $\mathfrak{I}$ un idéal de $\mathbb{G}$. Si $\mathfrak{I} = \{0\}$, alors $\mathfrak{I} = 0\mathbb{G}$. Supposons $\mathfrak{I} \neq \{0\}$. Soit

$$A = \{N(x) : x \in \mathfrak{I}, x \neq 0\}$$

L'ensemble A est une partie non vide de $\mathbb{N}$, il possède donc un plus petit élément. Soit $a \in \mathfrak{I}$ non nul tel que $N(a) = \min A$. Comme $\mathfrak{I}$ est un idéal, $a\mathbb{G} \subseteq \mathfrak{I}$. Inversement, soit $x \in \mathfrak{I}$. Effectuons la division euclidienne de x par a : il existe $(q, r) \in \mathbb{G}^2$ tel que $x = aq + r$ et $N(r) < N(a)$. On a $r = x - aq \in \mathfrak{I}$. Mais $N(r) < N(a) = \min A$, donc $N(r) \notin A$. Ainsi, $N(r) = 0$, d'où $r = 0$ et $x = aq \in a\mathbb{G}$. □

On vérifie facilement que pour tous $a, a' \in \mathbb{G}$, on a $a\mathbb{G} = a'\mathbb{G}$ si et seulement si a et a' sont associés. Explicitement, $a\mathbb{G} = (-a)\mathbb{G} = (ia)\mathbb{G} = (-ia)\mathbb{G}$ et ce sont les seules possibilités.

2.4 Plus grand diviseur commun

Proposition 6. *Soient $a, b \in \mathbb{G}$. Il existe $\delta \in \mathbb{G}$ tel que $a\mathbb{G} + b\mathbb{G} = \delta\mathbb{G}$. Un tel δ est unique à associé près.*

Démonstration. $a\mathbb{G} + b\mathbb{G}$ est un idéal de $\mathbb{G}$, d'où l'existence. Pour l'unicité, nous avons vu que $\delta\mathbb{G} = \delta'\mathbb{G}$ si et seulement si δ et δ' sont associés. □

Un tel δ est un *plus grand diviseur commun* (en abrégé pgcd) de a et b. Deux éléments a et b de $\mathbb{G}$ possèdent donc 4 pgcd, sauf si $a = b = 0$ (dans ce cas, le seul pgcd est 0). Lorsque δ est un

pgcd de a et b, nous noterons $\delta = a \wedge b$. Un et un seul des pgcd de a et b appartient à $\mathcal{R}$, c'est celui que nous privilégierons. Remarquons que le entiers naturels non nuls appartiennent à $\mathcal{R}$.

Nous dirons que a et b sont *premiers entre eux* lorsque $a \wedge b = 1$.

L'anneau $\mathbb{G}$ étant euclidien, toutes les propriétés du pgcd bien connues dans $\mathbb{Z}$ y restent vérifiées : algorithme d'Euclide, théorème de Bézout, lemme de Gauss, etc. Nous ne les détaillerons pas ici, les preuves sont en tous points identiques à celles qui sont faites dans $\mathbb{Z}$. Signalons tout de même le résultat suivant.

Proposition 7. *Soient $a, b \in \mathbb{Z}$. Le pgcd de a et b dans $\mathbb{Z}$ est aussi, à associé près, le pgcd de a et b dans $\mathbb{G}$.*

Démonstration. Soient $\delta \in \mathbb{G}$ le pgcd de a et b dans $\mathbb{G}$ et $\delta' \in \mathbb{Z}$ le pgcd de a et b dans $\mathbb{Z}$. Comme δ' divise a et b dans $\mathbb{Z}$ il les divise aussi dans $\mathbb{G}$. De là, δ' divise δ.

Écrivons $ua + vb = \delta'$ où $u, v \in \mathbb{Z}$. δ divise a et b dans $\mathbb{G}$, donc il divise $ua + vb = \delta'$ dans $\mathbb{G}$. Ainsi, δ et δ' sont associés dans $\mathbb{G}$. □

3 Primalité

3.1 Irréductibilité et primalité

Lorsqu'on cherche à définir la notion d'élément premier dans un anneau, on est amené à introduire deux concepts : l'*irréductibilité* et la *primalité*.

Définition 4. $p \in \mathbb{G}$ est *irréductible* si

- $p \notin \mathbb{U}$.
- Pour tous $a, b \in \mathbb{G}$, $p = ab \implies a \in \mathbb{U}$ ou $b \in \mathbb{U}$.

Définition 5. $p \in \mathbb{G}$ est *premier* si

- $p \neq 0$.
- $p \notin \mathbb{U}$.
- Pour tous $a, b \in \mathbb{G}$, $p|ab \implies p|a$ ou $p|b$.

Il s'avère que dans l'anneau $\mathbb{G}$, primalité et irréductibilité sont deux concepts équivalents. Commençons par un lemme facile.

Lemme 8. *Soient $a, p \in \mathbb{G}$. On suppose que p est irréductible et p ne divise pas a. Alors, p est premier avec a.*

Démonstration. Soit $\delta = a \wedge p$. Comme δ divise p, $\delta = 1$ ou $\delta = p$ (à associés près). Mais δ divise a et p ne divise pas a, donc $\delta \neq p$. Ainsi, $\delta = 1$. □

Proposition 9. *Soit $p \in \mathbb{G}$ non nul. p est irréductible si et seulement si p est premier.*

Démonstration. Supposons p premier. Soient $a, b \in \mathbb{G}$ tels que $p = ab$. On a $p|ab$ donc, comme p est premier, p divise a ou p divise b. Par exemple, $p|a$. Soit $c \in \mathbb{G}$ tel que $a = pc$. On a alors $p = ab = pcb$. Comme $p \neq 0$, $1 = cb$ donc $b \in \mathbb{U}$. Ainsi, p est irréductible.

Supposons p irréductible. Soient $a, b \in \mathbb{G}$ tels que $p|ab$. Supposons que p ne divise pas a. Par le lemme 8, a est premier avec p. Soit $c \in \mathbb{G}$ tel que $ab = pc$. On a $a|pc$ et a premier avec p donc, par le lemme de Gauss, a divise c. Soit $d \in \mathbb{G}$ tel que $c = ad$. On a alors $ab = pc = pad$. Comme p ne divise pas a, $a \neq 0$ et donc $b = pd$. Ainsi, p divise b. L'entier de Gauss p est donc premier. □

Remarquons que primalité $\implies$ irréductibilité n'utilise que la définition de la relation de divisibilité et l'intégrité de l'anneau. En revanche, irréductibilité $\implies$ primalité utilise le lemme de Gauss, qui est vérifié dans $\mathbb{G}$ parce que $\mathbb{G}$ est un anneau principal.

Remarque. Si $p \in \mathbb{Z}$, deux questions se posent : p est il premier en tant qu'élément de $\mathbb{Z}$? p est il premier en tant qu'élément de $\mathbb{G}$? Nous allons voir que ces deux questions sont liées, mais aussi qu'il n'y a pas équivalence. Pour lever toute ambiguïté, nous insisterons si besoin en disant « p est premier dans $\mathbb{Z}$ » ou « p est premier dans $\mathbb{G}$ ».

3.2 Sommes de deux carrés

Nous allons voir dans ce qui suit que **la** clé pour l'étude des entiers de Gauss premiers est la réponse à cette question : quels sont les entiers relatifs premiers dans $\mathbb{Z}$ qui sont la somme de deux carrés ?

Proposition 10. *Soit p un entier naturel impair. On suppose qu'il existe $a, b \in \mathbb{N}$ tels que $p = a^2 + b^2$. Alors, $p \equiv 1 \bmod 4$.*

Démonstration. Les carrés modulo 4 sont 0 et 1. De là, pour tous $a, b \in \mathbb{N}$, $a^2 + b^2$ est congru à 0, 1 ou 2 modulo 4. D'où le résultat puisque p est impair. □

Lemme 11. *Soit p un entier naturel premier congru à 1 modulo 4. Alors, -1 est un carré modulo p.*

Démonstration. Nous utilisons ici des résultats sur les résidus quadratiques. Ces résultats sont détaillés dans l'annexe. Si $a \in \mathbb{Z}$ n'est pas un multiple de p, alors a est un carré modulo p si et seulement si $a^{(p-1)/2} \equiv 1 \bmod p$. Comme $p \equiv 1 \bmod 4$, $(p-1)/2$ est pair et donc $(-1)^{(p-1)/2} = 1 \equiv 1 \bmod p$. □

Remarque. L'annexe fournit ici aussi les détails. Il est facile d'écrire un algorithme probabiliste qui calcule une racine carrée de -1 modulo p. Dans un premier temps, on trouve $a \in [\![1, p-1]\!]$ qui n'est pas un carré modulo p. Pour cela, il suffit de choisir a « au hasard ». Avec une probabilité $1/2$, a convient. On prend ensuite $r = a^{(p-1)/4}$ modulo p. On a alors

$$r^2 = a^{(p-1)/2} \equiv -1 \bmod p$$

Proposition 12. *Soit p un entier naturel premier congru à 1 modulo 4. Alors, p est la somme de deux carrés.*

Démonstration. Soit $r \in [\![0, p-1]\!]$ tel que $r^2 \equiv -1 \bmod p$. Un tel r existe par le lemme 11. Soit $\delta = a + ib = p \wedge (r + i)$, où le pgcd est évidemment un pgcd dans $\mathbb{G}$.

Par définition de r, p divise $r^2 + 1$ dans $\mathbb{Z}$, donc p divise $(r+i)(r-i)$ dans $\mathbb{G}$. En supposant un court instant que p est premier avec $r + i$ dans $\mathbb{G}$ alors, par le lemme de Gauss, p divise $r - i$. De là, $\frac{r}{p} - \frac{i}{p} \in \mathbb{G}$, contradiction. Ainsi, $\delta \neq 1$ (à associé près), donc $N(\delta) \neq 1$.

Comme δ divise $r+i$ dans $\mathbb{G}$, $N(\delta)$ divise $N(r+i) = r^2+1$ dans $\mathbb{Z}$. Remarquons que $(p-1)^2 \equiv 1 \bmod p$, donc $r \neq p-1$, donc $0 \leq r < p-1$. De là,

$$N(\delta) | r^2 + 1 < (p-1)^2 + 1 = p^2 + 2(1-p) < p^2$$

et donc $N(\delta) \neq p^2$.

Comme δ divise p dans $\mathbb{G}$, $N(\delta) = a^2 + b^2$ divise $N(p) = p^2$ dans $\mathbb{Z}$. Or, $N(\delta) \neq 1$ et $N(\delta) \neq p^2$, donc $N(\delta) = p$. Ainsi, $a^2 + b^2 = p$. □

Pour résumer ce qui précède, remarquons que $2 = 1^2 + 1^2$ est la somme de deux carrés. Un entier naturel p premier dans $\mathbb{Z}$ est donc la somme de deux carrés si et seulement si $p = 2$ ou $p \equiv 1 \bmod 4$.

3.3 Entiers relatifs premiers dans $\mathbb{G}$

Proposition 13. *Soit $p \in \mathbb{Z}$. L'entier p est premier dans $\mathbb{G}$ si et seulement si p est premier dans $\mathbb{Z}$ et $|p| \equiv 3 \bmod 4$.*

Démonstration. Tout d'abord, si p est composé dans $\mathbb{Z}$ alors p l'est évidemment dans $\mathbb{G}$. Nous supposons dorénavant p premier dans $\mathbb{Z}$. On a $2 = (1+i)(1-i)$ donc 2 n'est pas premier dans $\mathbb{G}$. De plus, p est premier dans $\mathbb{G}$ si et seulement si $-p$ l'est. Nous pouvons donc supposer dans la suite que $p \geq 3$. L'entier p est donc congru à 1 ou à 3 modulo 4.

Supposons $p \equiv 1 \bmod 4$. Par la proposition 12, il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$. De là, $p = (a+ib)(a-ib)$ n'est pas premier dans $\mathbb{G}$.

Inversement, supposons que p n'est pas premier dans $\mathbb{G}$. Il existe donc $x, y \in \mathbb{G}$ non inversibles tels que $p = xy$. En passant aux normes, il vient $p^2 = N(x)N(y)$. Comme p est premier dans $\mathbb{Z}$ et $N(x), N(y) \geq 2$, on a $N(x) = N(y) = p$. De là $p = x\overline{x}$. Posons $x = a + ib$ où $a, b \in \mathbb{Z}$. On a $a^2 + b^2 = p$. L'entier p est la somme de deux carrés donc, par la proposition 10, $p \equiv 1 \bmod 4$. □

3.4 Se ramener aux entiers relatifs

Maintenant que nous connaissons les entiers relatifs qui sont premiers dans $\mathbb{G}$, nous pouvons examiner le cas général. Nous allons voir que si $x \in \mathbb{G}$, l'étude de la primalité de x se ramène à celle de $N(x)$.

Proposition 14. *Soit $x = a + ib \in \mathbb{G}$.*

- *Si x est associé à un entier relatif, alors x est premier si et seulement si $|x|$ est premier dans $\mathbb{Z}$ et $|x| \equiv 3 \bmod 4$.*
- *Sinon, x est premier si et seulement si $N(x)$ est premier dans $\mathbb{Z}$.*

Démonstration.

- Supposons x associé à un entier relatif p. On a $x = \pm p$ ou $x = \pm ip$, et $|x| = |p|$. Il suffit d'appliquer la proposition 13.
- Supposons que x n'est pas associé à un entier relatif.

  Supposons x composé dans $\mathbb{G}$. Soient $a, b \in \mathbb{G}$ non inversibles tels que $x = ab$. En passant aux normes, $N(x) = N(a)N(b)$. Comme $N(a)$ et $N(b)$ sont différents de 1, $N(x)$ est composé dans $\mathbb{Z}$.

  Inversement, supposons x premier dans $\mathbb{G}$. On a $N(x) = x\overline{x}$, donc x divise $N(x)$ dans $\mathbb{G}$. Par le lemme d'Euclide, x divise l'un des facteurs premiers de $N(x)$ dans $\mathbb{Z}$. Soit p un tel facteur premier. On a $x|p$, donc aussi $\overline{x}|\overline{p} = p$, d'où $N(x) = x\overline{x}|p^2$. De là, $N(x) = 1$, p ou p^2. Comme x est premier, $N(x) \neq 1$. Il reste à voir que $N(x) \neq p^2$. Supposons le contraire. Écrivons $p = xy$ où $y \in \mathbb{G}$. En passant aux normes,

  $$p^2 = N(p) = N(x)N(y) = p^2 N(y)$$

  donc $N(y) = 1$, c'est à dire y est inversible. De là, x et p sont associés, contradiction.

□

Pour prendre les choses « à l'envers » soit p un entier naturel premier impair.

- Si $p \equiv 3 \bmod 4$, alors $\pm p$ et $\pm ip$ sont premiers dans $\mathbb{G}$.
- Si $p \equiv 1 \bmod 4$, alors $p = a^2 + b^2$ où $a, b \in \mathbb{Z}$. Les entiers de Gauss $\pm(a \pm ib)$ et $\pm(b \pm ia)$ sont alors premiers dans $\mathbb{G}$.
- Tous les entiers de Gauss premiers sont obtenus de cette façon.

Le cas numéro 2 mérite que l'on se penche sur des questions d'unicité.

Proposition 15. *Soit p un entier naturel premier dans $\mathbb{Z}$ congru à 1 modulo 4. Il existe exactement deux couples $(a, b) \in \mathbb{N}^2$ tels que $p = a^2 + b^2$. Si (a, b) est l'un des couples, l'autre est (b, a).*

Démonstration. On a $p = x\overline{x}$ où x est un entier de Gauss premier.

Supposons $p = x\overline{x} = y\overline{y}$ où y est premier dans $\mathbb{G}$. x divise $y\overline{y}$ et x est premier, donc x divise y ou x divise $\overline{y}$. Par exemple, x divise y. Soit $z \in \mathbb{G}$ tel que $y = xz$. On a $x\overline{x} = z\overline{z}x\overline{x}$, d'où $N(z) = z\overline{z} = 1$. Ainsi, x et y sont associés.

Ainsi, les seuls diviseurs premiers de p sont x et $\overline{x}$. Ces deux diviseurs ont chacun un unique associé dans $\mathcal{R}$. Il y a donc deux couples $(a, b) \in \mathbb{N}^2$ tels que $p = a^2 + b^2$. Pour terminer,

remarquons que $a \neq b$ car sinon, $p = 2a^2$, ce qui contredit $p \equiv 1 \bmod 4$. De plus, si (a, b) convient alors, par symétrie, (b, a) convient aussi. □

La figure ci-dessous représente les entiers de Gauss premiers de module inférieur ou égal à 100.

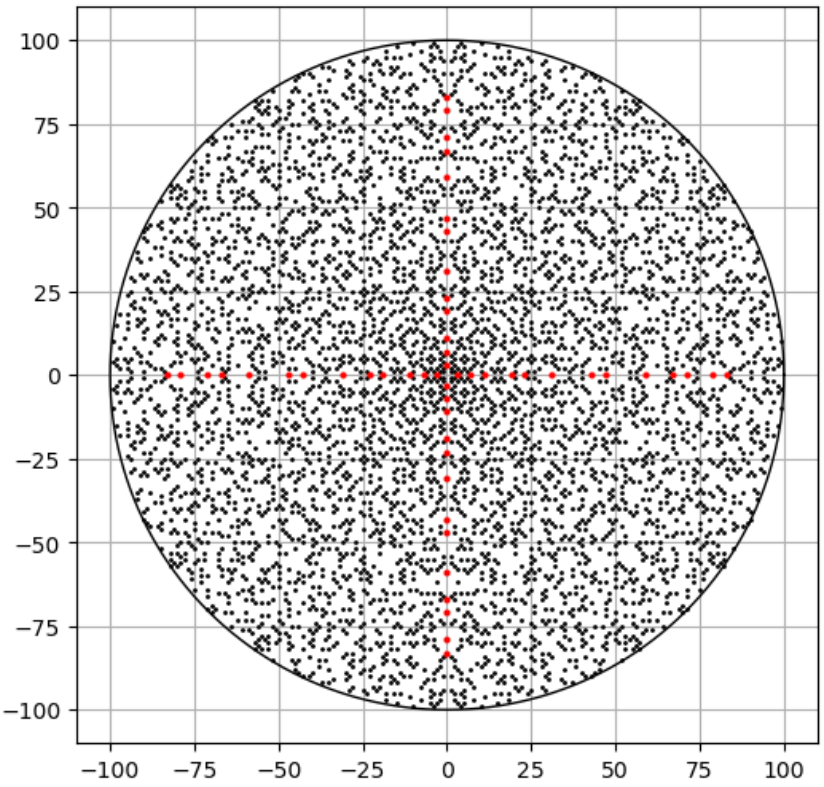

FIGURE 1 – Les entiers de Gauss premiers de module inférieur à 10^2

4 Factorialité

4.1 Introduction

L'anneau $\mathbb{G}$ est un anneau principal, il est donc aussi *factoriel* : tout élément non nul de $\mathbb{G}$ s'écrit de façon « unique » comme un produit d'entiers de Gauss premiers. Nous allons préciser un peu la question de l'unicité.

Notons $\mathcal{P}_+$ l'ensemble des entiers de Gauss premiers qui appartiennent à $\mathcal{R}$.

4.2 Le théorème de décomposition unique

Lemme 16. *Soit $x \in \mathbb{G} \setminus \mathbb{U}$. L'entier de Gauss x possède un diviseur $p \in \mathcal{P}_+$.*

Démonstration. Procédons par récurrence sur $N(x)$. Les seuls entiers de Gauss de norme 2 sont $\pm 1 \pm i$. Il sont tous associés à $1+i$ qui appartient à $\mathcal{P}_+$. Soit maintenant $n \geq 3$. Supposons la

propriété vérifiée pour tous les entiers de Gauss non inversibles de norme strictement inférieure à n. Soit $x \in \mathbb{G} \setminus \mathbb{U}$ de norme n. Si x est premier, alors, par le lemme précédent, un (et un seul) des associés de x appartient à $\mathcal{P}_+$. Cet associé divise x. Si x n'est pas premier, alors $x = ab$ où $a, b \in \mathbb{G}$ ne sont pas inversibles. On a $n = N(x) = N(a)N(b) > N(a)$. Par l'hypothèse de récurrence, il existe $p \in \mathcal{P}_+$ tel que p divise a. Comme a divise x, p divise x. □

Proposition 17. *Soit $x \in \mathbb{G}$ non nul. L'entier de Gauss x s'écrit de façon unique*

$$x = u \prod_{p \in \mathcal{P}_+} p^{\nu_p}$$

où $u \in \mathbb{U}$ et les ν_p sont des entiers naturels presque tous nuls.

Démonstration. Montrons l'existence par récurrence forte sur $N(x)$. Si $N(x) = 1$, il suffit de poser $u = x \in \mathbb{U}$ et pour tout $p \in \mathcal{P}_+$, $\nu_p = 0$. Soit $n > 1$. Supposons l'existence de la décomposition assurée pour tous les entiers de Gauss non nuls de norme strictement inférieure à n. Soit $x \in \mathbb{G}$ de norme n. Par le lemme précédent, il existe $p_0 \in \mathcal{P}_+$ qui divise x. On a $x = p_0 x'$ où $x' \in G$, $x' \neq 0$ et $N(x') < N(x)$. Par l'hypothèse de récurrence,

$$x' = u \prod_{p \in \mathcal{P}_+} p^{\nu'_p}$$

où $u \in \mathbb{U}$ et les ν'_p sont des entiers naturels presque tous nuls. On a alors

$$x = u \prod_{p \in \mathcal{P}_+} p^{\nu_p}$$

où $\nu_p = \nu'_p$ si $p \neq p_0$ et $\nu_{p_0} = \nu'_{p_0} + 1$.

Passons à l'unicité. Supposons

$$(\star)\ u \prod_{p \in \mathcal{P}_+} p^{\nu_p} = u' \prod_{p \in \mathcal{P}_+} p^{\nu'_p}$$

où $u, u' \in \mathbb{U}$ et les ν_p, ν'_p sont des entiers naturels presque tous nuls. Soit $p_0 \in \mathcal{P}_+$. L'entier de Gauss p_0 est premier avec tous les ν_p, $p \neq p_0$, donc $p_0^{\nu_{p_0}}$ est premier avec le produit des $p^{\nu'_p}$, $p \neq p_0$. En appliquant le lemme de Gauss, on en déduit que $p_0^{\nu_{p_0}}$ divise $p_0^{\nu'_{p_0}}$. De même, $p_0^{\nu'_{p_0}}$ divise $p_0^{\nu_{p_0}}$. Ainsi, il existe $v \in \mathbb{U}$ tel que

$$p_0^{\nu'_{p_0}} = v p_0^{\nu_{p_0}}$$

En passant aux normes,

$$N(p_0)^{\nu'_{p_0}} = N(p_0)^{\nu_{p_0}}$$

Cette égalité entre entiers naturels entraîne $\nu'_{p_0} = \nu_{p_0}$. Ainsi, pour tout $p \in \mathcal{P}_+$, $\nu'_p = \nu_p$. En reportant dans $(\star)$, on obtient pour terminer $u' = u$. □

4.3 La décomposition en pratique

Dans ce paragraphe, nous allons montrer que pour décomposer un entier de Gauss en produit de nombres de Gauss premiers, il suffit de savoir décomposer un entier relatif en produit d'entiers relatifs premiers.

Soit $x \in \mathbb{G} \setminus \{0\}$. Notons $\mathcal{P}_\mathbb{Z}$ l'ensemble des entiers naturels premiers. Écrivons

$$x = u \prod_{p \in \mathcal{P}_+} p^{\nu_p}$$

où $u \in \mathbb{U}$ et les ν_p sont des entiers naturels presque tous nuls. On a

$$N(x) = \prod_{p \in \mathcal{P}_+} N(p)^{\nu_p}$$

Notons $\mathcal{P}_\mathbb{Z}$ l'ensemble des entiers naturels premiers. Comme $N(x) \in \mathbb{N}^*$, on peut décomposer $N(x)$ en produit d'entiers naturels premiers. Supposons connue cette décomposition :

$$N(x) = \prod_{q \in \mathcal{P}_\mathbb{Z}} q^{\mu_q}$$

où les μ_q sont des entiers naturels presque tous nuls.

Il s'agit de déterminer les ν_p en fonction des μ_q. Discutons sur $q \in \mathcal{P}_\mathbb{Z}$.

- Tout d'abord, $\nu_{1+i} = \mu_2$.
- Si q est un entier naturel premier congru à 3 modulo 4, alors $q \in \mathcal{P}_+$ et $2\nu_p = \mu_q$.
- Si q est un entier naturel premier congru à 1 modulo 4, alors q s'écrit de façon quasi-unique $q = a^2 + b^2$ où $a, b \in \mathbb{N}^*$. L'entier q est la norme de **deux** éléments de $\mathcal{P}_+$: $q = N(p) = N(p')$ où $p = a + ib$ et $p' = b + ia$. On a dans ce cas $\nu_p + \nu_{p'} = \mu_q$. Si $\mu_q \neq 0$, on peut, algorithmiquement, effectuer des divisions successives de x par p pour obtenir ν_p. On en déduit alors $\nu_{p'}$.

Une fois déterminés les ν_p, on obtient u par une simple division.

5 Annexe - Résidus quadratiques

Soit p un entier naturel premier impair. L'anneau $\mathbb{Z}_p$ des entiers modulo p est un corps. Notons $\mathbb{Z}_p^\times$ le groupe des éléments non nuls de $\mathbb{Z}_p$. Considérons l'application $f : \mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times$ définie par $f(x) = x^2$. L'application f est un endomorphisme du groupe $\mathbb{Z}_p^\times$. L'ensemble $Q_p = f(\mathbb{Z}_p^\times)$ est un sous-groupe de $\mathbb{Z}_p^\times$, l'ensemble des *résidus quadratiques* (modulo p).

Proposition 18. $|Q_p| = (p-1)/2$.

Démonstration. Considérons la relation $\sim$ sur $\mathbb{Z}_p^\times$ définie par $a \sim b$ si et seulement si $f(a) = f(b)$. Cette relation est clairement une relation d'équivalence. De plus, $f(a) = f(b)$ si et seulement si $(a-b)(a+b) = 0$, ou encore $a = \pm b$. Comme p est impair, $-b \neq b$. Les classes modulo $\sim$ sont donc de cardinal 2. Par le lemme des bergers,

$$2|f(\mathbb{Z}_p^\times)| = |\mathbb{Z}_p^\times|$$

d'où le résultat. □

Lemme 19. *Pour tout $x \in \mathbb{Z}_p^\times$, $x^{(p-1)/2} = \pm 1$.*

Démonstration. Soit $x \in \mathbb{Z}_p^\times$. Soit $y = x^{(p-1)/2}$. Par le petit théorème de Fermat, $y^2 = x^{p-1} = 1$. On a donc $(y-1)(y+1) = 0$, d'où $y = \pm 1$. □

Lemme 20. *Soit $x \in \mathbb{Z}_p^\times$. Si $x \in Q_p$, alors $x^{(p-1)/2} = 1$. Si $x \notin Q_p$, alors $x^{(p-1)/2} = -1$.*

Démonstration. Soit $x \in Q_p$. Il existe $a \in \mathbb{Z}_p^\times$ tel que $x = a^2$. De là, par le petit théorème de Fermat,

$$x^{(p-1)/2} = a^{p-1} = 1$$

Considérons le polynôme

$$P = X^{(p-1)/2} - 1$$

Le polynôme P, de degré $(p-1)/2$, a au plus $(p-1)/2$ racines. Or, les éléments de Q_p sont $(p-1)/2$ racines de P. Les racines de P sont donc les éléments de Q_p. Pour tout $x \notin Q_p$, x n'est donc pas racine de P, c'est à dire $x^{(p-1)/2} \neq 1$ et donc $x^{(p-1)/2} = -1$. □